CLAIM AMENDMENTS

Claims 1-3, 5-7 and 9-40 are pending. Claim 23 is currently amended herein to correct for a misspelled word.

1   1. (previously presented) A system for preventing an illegal copy of digital content, said

2   system receiving and decrypting encrypted digital content and reproducing the digital content,

3   comprising:

4   a certificate authority for generating manufacturer key information and generating first key

5   information for giving an authorization to supply said encrypted digital content;

6   a portable terminal supplier supplying a portable terminal, said portable terminal supplier

7   outputting a first registration request signal to said certificate authority and receiving the

8   manufacturer key information generated by said certificate authority in accordance with the first

9   registration request signal, said portable terminal supplier imbedding the manufacturer key

10   information in said portable terminal;

11   a content supplier transmitting a second registration request signal to the certificate authority,

12   said certificate authority and said content supplier sharing a first secret channel, said content supplier

13   receiving and storing said first key information from the certificate authority through said first secret

14   channel for supplying said encrypted digital content, said content supplier generating and outputting

15   second key information for giving an authorization to receive and reproduce said encrypted digital

16   content;

17   a personal computer outputting a third registration request signal to the content supplier for

18 obtaining said second key information, said personal computer having public key information of said

19 certificate authority, said personal computer and said content supplier sharing a second secret

20 channel, said personal computer verifying said first key information inputted from the content

21 supplier by using said public key information of said certificate authority and receiving the second

22 key information through said second secret channel, said personal computer receiving said encrypted

23 digital content through said second secret channel; and

24 said portable terminal manufactured by said portable terminal supplier for reproducing said

25 digital content, said portable terminal transferring the imbedded manufacturer key information to

26 said content supplier through said personal computer to be verified by said content supplier, said

27 portable terminal and said personal computer sharing a third secret channel for transferring said

28 encrypted digital content between said portable terminal and said personal computer.

1 2. (previously presented) The system as claimed in claim 1, wherein the certificate authority

2 generates a first channel key shared with the content supplier to form said first secret channel, the

3 first key information is encoded by said first channel key and then transferred to said content

4 supplier, and said content supplier decodes the encoded first key information by said first channel

5 key.

1 3. (previously presented) The system as claimed in claim 1, wherein the content supplier

2 generates a second channel key shared with the personal computer to form said second secret

3 channel, and the second key information is encoded by said second channel key, and then transferred

4   to said personal computer.

1   5. (previously presented) A system for preventing an illegal copy of digital content,

2   comprising:

3   a certificate authority for generating manufacturer key information comprising a

4   manufacturer key and a manufacturer key data in response to a first registration request signal

5   inputted from an external source, generating first key information for giving an authorization to

6   supply said digital content, said certificate authority generating a token to make an information table,

7   said information table comprising a first table containing the manufacturer key data, the

8   manufacturer key, and an identifier corresponding to the manufacturer key, and a second table

9   containing said identifier, token information encrypted by said manufacturer key, and said token;

10   a content supplier transmitting a second registration request signal to the certificate authority

11   for supplying said digital content, said certificate authority and said content supplier sharing a first

12   secret channel, said content supplier receiving and storing said first key information and said second

13   table from the certificate authority through said first secret channel, said content supplier generating

14   second key information;

15   first content output means for outputting the digital content, said first content output means

16   sending a third registration request signal to the content supplier for downloading said digital content

17   from said content supplier, said first content output means having public key information of said

18   certificate authority, said first content output means and said content supplier sharing a second secret

19   channel, said first content output means verifying said first key information inputted from the content

20   supplier by using said public key information of said certificate authority and receiving the second

21   key information through said second secret channel, said first content output means extracting the

22   manufacturer key information from said second table, and encoding and outputting the manufacturer

23   key information; and

24   said second content output means for recording and reproducing said digital content, said

25   second content output means storing the manufacturer key information, said second output means

26   transferring said manufacturer key information to said content supplier through said first content

27   output means to be verified by said content supplier, said second content output means receiving said

28   manufacturer key information of said second table from said first content output means to decide if

29   the manufacturer key is authenticated, said second content output means and said first content output

30   means sharing a third secret channel for transferring said digital content between said second content

31   output means and said first content output means.

1   6. (previously presented) The system claimed in claim 5, wherein a content storage means

2   is further included in at least one of said second content output means and said first content output

3   means, and said content storage means stores said digital content.

1   7. (previously presented) The system claimed in claim 5, wherein the certificate authority

2   generates a first channel key shared with the content supplier to form said first secret channel, the

3   first key information is encoded by said first channel key and then transferred to said content

4   supplier, and said content supplier decodes the encoded first key information by said first channel

5   key.

1   9. (previously presented) The system claimed in claim 5, wherein the content supplier

2   generates a second channel key shared with the first content output means to form said second secret

3   channel, and the second key information is encoded by the second channel key, and then transferred

4   to said first content output means.

1   10. (previously presented) The system claimed in claim 5, wherein the token is randomly

2   generated by the certificate authority.

1   11. (previously presented) The system claimed in claim 7, wherein the first content output

2   means generates a third channel key shared with the second content output means to form said third

3   secret channel, and the first content output means encodes the third channel key with said token

4   inputted from the content supplier and transmits the third channel key to the second content output

5   means.

1   12. (previously presented) The system claimed in claim 11, the second content output means

2   decodes the encoded token transmitted from the first content output means by using the stored

3   manufacturer key, decodes and stores the third channel key by using said token.

1   13. (previously presented) The system claimed in claim 11, further comprised of:

2   said first content output means including a database which has reproduction data of the

3   digital content downloaded from the content supplier, said first content output means encoding the

4   database by using the third channel key for storage, interpreting the reproduction data of the digital

5   content by using the third channel key to thereby judge if an illegal copy of the digital content is

6   performed; and

7   said second content output means receiving said reproduction data from said first content

8   output means, updating the reproduction data whenever any content downloading or uploading

9   session between said first content output means and said second content output means occurs, and

10   transmitting the updated reproduction data of the digital content to the first content output means.

1   14. (previously presented) The system claimed in claim 13, wherein the database is separated

2   with an identifier data area of the digital content, an updated token data area, a data area for a present

3   state of the digital content, and a reproduction control data area, and has the corresponding data.

1   15. (previously presented) The system claimed in claim 14, wherein the data area for the

2   present state of the digital content comprises:

3   first data indicating that the digital content is downloaded in a copy form from the first

4   content output means to the second content output means;

5   second data indicating that the digital content is downloaded in a transmission form from the

6   first content output means to the second content output means; and

7   third data indicating that the digital content is downloaded and uploaded between the first

8   content output means and the second content output means.

1   16. (previously presented) The system claimed in claim 14, wherein the reproduction control

2   data area of the digital content includes:

3   fourth data for reproduction times of the digital content;

4   fifth data for a reproduction expiration period of the digital content; and

5   sixth data for an amnesty period of the digital content.

1   17. (previously presented) A system for protecting a illegal copy, comprising:

2   a terminal receiving a physical address of a bad sector of a storage medium, said terminal

3   generating a random number and storing said random number in a spare area of said storage medium,

4   said terminal having a secret channel key, said terminal function-processing said physical address,

5   said random number and said secret channel key to obtain a processed value, said terminal

6   encrypting a header of the digital content by the processed value; and

7   said storage medium transmitting said physical address of the bad sector, storing said random

8   number as a key value generated from said terminal, storing as a sector data the encrypted digital

9   content and the header of the digital content encrypted by using the processed value.

1   18.   (previously presented) A system for protecting an illegal copy of digital content,

2   comprising:

3   a certificate authority for generating manufacturer key information and generating first key

4 information for giving an authorization to supply said digital content;

5 a terminal supplier supplying a terminal, said terminal supplier outputting a first registration

6 request signal to said certificate authority and receiving the manufacturer key information generated

7 by said certificate authority in accordance with the first registration request signal, said terminal

8 supplier embedding the manufacturer key information in said terminal;

9 a content supplier sending a second registration request signal to the certificate authority, said

10 certificate authority and said content supplier sharing a first secret channel, said content supplier

11 receiving and storing said first key information from the certificate authority through said first secret

12 channel for supplying said digital content, said content supplier generating and outputting second

13 key information for giving an authorization to receive and reproduce said digital content from said

14 second key information;

15 a personal computer sending a third registration request signal to the content supplier for

16 obtaining said second key information, said personal computer having public key information of said

17 certificate authority, said personal computer and said content supplier sharing a second secret

18 channel, said personal computer verifying said first key information inputted from the content

19 supplier by using said public key information of said certificate authority and receiving the second

20 key information through said second secret channel, said personal computer receiving said digital

21 content through said second secret channel;

22 said terminal manufactured by said terminal supplier for reproducing said digital content and

23 reading a storage medium, said terminal transferring the embedded manufacturer key information

24 to said content supplier through said personal computer to be verified by said content supplier, said

25 terminal and said personal computer sharing a third secret channel for transferring said digital

26 content between said terminal and said personal computer, said terminal receiving and function-

27 processing a physical address of a bad sector of the storage medium, a random number generated and

28 stored in a spare area of said terminal and a secret channel key generated in said terminal to obtain

29 a processed value, said terminal encrypting a header of the digital content with the processed value;

30 and

31 said storage medium transmitting said physical address of the bad sector, storing said random

32 number as a key value generated from said terminal, storing as a sector data the encrypted header of

33 the digital content and encrypted header information encrypted by using the result of function

34 processing.

1 19. (previously presented) The system claimed in claim 18, wherein the certificate authority

2 generates a first channel key shared with the content supplier to form said first secret channel, the

3 first key information is encoded by said first channel key and then transferred to said content

4 supplier, and said content supplier decodes the encoded first key information by said first channel

5 key, the content supplier generates a second channel key shared with the personal computer to form

6 said second secret channel, and the second key information is encoded by the second channel key,

7 and then transferred to said personal computer, and the personal computer generates a third channel

8 key shared with the terminal to form said third secret channel, and the personal computer encodes

9 the third channel key with said token inputted from the content supplier and transmits the third

10 channel key to the terminal.

1   20. (previously presented) The system claimed in claim 19, further comprised of:

2   said personal computer having a database which comprises reproduction data of the digital

3   content downloaded from the content supplier, the database encoded by using the third channel key,

4   said personal computer interpreting the digital content by using the third channel key to decide if an

5   illegal copy of the digital content is performed; and

6   said terminal receiving said reproduction data from said personal computer, updating the

7   reproduction data whenever any content downloading or uploading session between said terminal

8   and said personal computer occurs, and transmitting the updated reproduction data to the personal

9   computer.

1   21. (previously presented) The system claimed in claim 20, wherein the database is separated

2   with an identifier data area of the digital content, an updated token data area, and a data area for a

3   present state of the digital content, and a reproduction control data area.

1   22. (previously presented) The system claimed in claim 21, wherein the data area for the

2   present state of the digital content includes first data indicating that the digital content is downloaded

3   in a copy form from the personal computer to the terminal. second data indicating that the digital

4   content is downloaded in a transmission form from the personal computer to the terminal, and third

5   data indicating that the digital content is downloaded and uploaded between the personal computer

6   and the terminal, and the reproduction control data area of the digital content includes fourth data

7   for reproduction times of the digital content, fifth data for a reproduction expiration period of the

8   digital content; and sixth data for an amnesty period of the digital content.

1   23. (currently amended) A server for preventing an unauthorized copy of digital content,

2   said server comprising:

3   a first cryptosystem verifying public key information of a content provider by using public

4   key information embedded in said server to check whether said content provider has an authorization

5   to supply said digital content, said server establishing a second secure channel to said content

6   provider to download said digital content from said content provider;

7   a second cryptosystem encrypting and ~~transfering~~ transferring manufacturer key information

8   embedded in a terminal linked to said server from said terminal to said content provider to be

9   verified by said content provider, said server establishing a third secure channel to said terminal after

10   the validation of the manufacturer key information, said server ~~transfering~~ transferring a token of

11   said content provider to said terminal through said second secure channel and said third secure

12   channel; and

13   a secure check-in and check-out system for checking a validation of said digital content, said

14   secure check-in and check-out system comprising a right management system having a right

15   management database, wherein information of said digital content corresponding to said right

16   management database is registered to said right management system, said right management database

17   is updated whenever said digital content is downloaded or uploaded between said server and said

18   terminal to check if an unauthorized copy of said digital content is performed.

-12-

24. (previously presented) The server of claim 23, wherein said second secure channel is established by executing a handshaking protocol to get an ephemeral shared key by utilizing Elliptic curve based key exchanging protocol.

25. (previously presented) The server of claim 23, wherein said third secure channel is established by a third secret channel key generated in one of said server and said terminal.

26. (previously presented) The server of claim 25, wherein said right management database comprises reproduction data of said digital content, said server encodes said reproduction data by using said third secure channel key, and said server checks said reproduction data by using said third secure channel key.

27. (previously presented) The server of claim 25, wherein said right management database comprises an identifier data area of the digital content, an updated token data area, a data area for a present state of the digital content, and a reproduction control data area.

28. (previously presented) The server of claim 27, wherein the data area for the present state of the digital content comprises:

first data indicating that the digital content is downloaded in a copy form from said server to said terminal;

5   second data indicating that the digital content is downloaded in a transmission form from said

6   server to said terminal; and

7   third data indicating that the digital content is downloaded and uploaded between said server

8   and said terminal.

1   29. (previously presented) The server of claim 27, wherein the reproduction control data

2   area of the digital content comprises:

3   fourth data indicating reproduction times of the digital content;

4   fifth data indicating a reproduction expiration period of the digital content; and

5   sixth data indicating an amnesty period of the digital content.

1   30. (previously presented) The server of claim 27, wherein said digital content has a first file

2   format comprises:

3   a plain header comprising a title identifier, a content description field, and an algorithm

4   identifying field from which said server finds out an encryption algorithm and a secret key of said

5   server;

6   a secret header comprising a device identifier to be compared with an identifier of said server,

7   an indicator of a source origination of said digital content, a right management field including data

8   to be registered to said right management system, and a content encryption key for recovering said

9   digital content encrypted by said content encryption key; and

10   a file body comprising said digital content encrypted by using said content encryption key.

1   31. (previously presented) The server of claim 30, further comprising:

2   an applied program interface confirming a validity of an input and extracting first information

3   from said input;

4   an import control layer receiving said first information from said applied program interface,

5   said import control layer reconstructing said first information into said first file format; and

6   a terminal interface authenticating said terminal by checking whether said terminal has a

7   correct identifier and said third secret channel key.

1   32. (previously presented) A terminal, comprising:

2   manufacturer key information embedded in said terminal; and

3   a symmetric key cryptosystem preventing an unauthorized copy of digital content by

4   responding to reception of said manufacturer key information by a server by establishing a secure

5   registration of said terminal with said server, with said terminal establishing a third secure channel

6   to said server and said terminal receiving a token from said server through said third secure channel

7   to reproduce said digital content provided by said server.

1   33. (previously presented) The terminal of claim 32, further comprising:

2   a public key cryptosystem, wherein said terminal verifies public key information of said

3   server by using public key information embedded in said terminal to check whether said server has

4   an authorization to download said digital content to said terminal.

1   34. (previously presented) The terminal of claim 32, wherein said terminal generates update

2   token data whenever said digital content is downloaded or uploaded between said terminal and said

3   server to check if an unauthorized copy of said digital content is performed.

1   35. (previously presented) The terminal of claim 34, wherein said third secure channel is

2   established by a third secret channel key.

1   36. (previously presented) The terminal of claim 35, wherein said update token data are

2   encoded and decoded by said third secret channel key.

1   37. (previously presented) The terminal of claim 32, wherein said digital content has a first

2   file format comprising:

3   a plain header comprising a title identifier, a content description field, and an algorithm

4   identifying field;

5   a secret header comprising a device identifier, an indicator of a source origination of said

6   digital content, a right management field, and a content encryption key for recovering said digital

7   content encrypted by said content encryption key; and

8   a file body comprising said digital content encrypted by said content encryption key.

1   38. (previously presented) The terminal of claim 37, wherein said terminal is able to write

2   said digital content encrypted by said content encryption key on a storage medium, recover said

3   secret header, and reencrypt said digital content by using an unique identifier in said storage medium,

4   and, if said storage medium does not have said unique identifier in said storage medium, said

5   terminal is able to write said digital content encrypted by said content encryption key on said storage

6   medium, recover said secret header, reencrypt said digital content by using a randomly generated

7   key, and encrypt and write said randomly generated key on a hidden area of said storage medium by

8   using a common secret key embedded in said terminal.

1   39. (previously presented) The terminal of claim 37, wherein said terminal has an import

2   control layer to convert an analog input to said digital content having said first file format.

1   40. (previously presented) The terminal of claim 38, wherein said unique identifier is a

2   physical address of a bad sector of said storage medium, said terminal has a random number

3   generator to generate a random number and stores said random number in a spare area of said storage

4   medium, and said terminal has a function-processor function-processing said physical address, said

5   random number and said third secure channel key to obtain a processed value, and said terminal

6   encrypts said digital content with the processed value.